Verifying temporal properties using explicit approximants: completeness for context-free processes

Schöpp, U., & Simpson, A. (2002). Verifying temporal properties using explicit approximants: completeness for context-free processes. In Foundations of Software Science and Computation Structures. (pp. 372-386). (Lecture Notes in Computer Science). Springer Berlin / Heidelberg. doi: 10.1007/3-540-45931-6_26

Verifying Temporal Properties using Explicit Approximants: Completeness for Context-free Processes

Ulrich Schöpp
Ulrich.Schoepp@ed.ac.uk

Alex Simpson
Alex.Simpson@dcs.ed.ac.uk

LFCS, Division of Informatics, University of Edinburgh
JCMB, King's Buildings, Edinburgh, EH9 3JZ

Abstract

We present a sequent calculus for formally verifying modal μ-calculus properties of concurrent processes. Building on work by Dam and Gurov, the proof system contains rules for the explicit manipulation of fixed-point approximants. We develop a new syntax for approximants, incorporating, in particular, a mechanism for approximant modification. We make essential use of this feature to prove our main result: the sequent calculus is complete for establishing arbitrary μ-calculus properties of context-free processes.

1 Introduction

Concurrent processes lie at the heart of many critical applications in computer science, and often have a rich and complex behaviour. So it is very desirable to ensure that such systems work correctly. Moreover, many correctness requirements are conveniently expressed using temporal logic. Thus one seeks methods of establishing relations of the form $p \models \varphi$, stating that process p satisfies temporal property φ.

For finite state systems, this problem can be addressed automatically by model checking. However, many concurrent processes are infinite state (at least potentially), and for such systems the verification problem is, in general, undecidable. In the face of undecidability, one has to settle for finding sound but necessarily incomplete methods for establishing correctness assertions. Because of incompleteness in general, the best one can hope for is to obtain partial completeness results for such methods, e.g. completeness with respect to restricted classes of processes.

In this paper, we provide a proof system for establishing correctness assertions $p \models \varphi$, where φ is a formula in the modal μ-calculus [13]. We prove the soundness of the system, Theorem 1, and illustrate its workings with an example derivation of a μ-calculus property with non-trivial fixed-point alternation. Following [16], the proof system can be adapted to processes in any process algebra with a GSOS-specified operational semantics [1]. Our main result, Theorem 2, is a restricted completeness result: the proof system is complete for establishing arbitrary μ-calculus properties of context-free processes, see e.g. [2]. As far as we know, this is the first completeness result for a general purpose proof system (i.e. one not tailored in advance to any one specific class of processes) with respect to a significant class of infinite state processes.

Motivation and previous work

The proof system we introduce is a sequent calculus in which sequents have the form $\Gamma \vdash \Delta$, where Γ and Δ are sets of assertions. As usual, a derivation of $\Gamma \vdash \Delta$ will establish that if all the assertions in Γ hold then so does at least one assertion in Δ. The principal assertion form is $p : \varphi$, which is the syntactic expression of the relation $p \models \varphi$. The sequent-based formalism has a number of virtues:

1. Ordinary verification goals are expressed by sequents of the form $\vdash p : \varphi$.

2. More generally, by allowing process variables, *modular* verification goals can be expressed by sequents of the form

$$x_1 : \psi_1,\ \ldots,\ x_n : \psi_n \vdash p(x_1, \ldots, x_n) : \varphi. \tag{1}$$

   Such a sequent states that the process p satisfies φ whenever its parameters $x_1, \ldots, x_n$ are instantiated with processes satisfying $\psi_1, \ldots, \psi_n$ respectively.

3. Such modularity goals can be used to support *compositional* reasoning. Using the familiar cut and substitution rules from sequent calculus, one obtains a derived rule:[1]

$$\frac{\vdash p(q_1, \ldots, q_n) : \varphi}{\vdash q_1 : \psi_1 \qquad \ldots \qquad \vdash q_n : \psi_n \qquad x_1 : \psi_1,\ \ldots,\ x_n : \psi_n \vdash p(x_1, \ldots, x_n) : \varphi}$$

   This rule reduces the goal of establishing a property φ of a compound process $p(q_1, \ldots, q_n)$ to the subgoals of establishing properties of its components $q_1, \ldots, q_n$ together with a further modularity subgoal justifying the decomposition.

4. The proof system also supports a direct *structural* form of reasoning. The main inference rules decompose logical connectives on the left and right of sequents in the familiar Gentzen style, allowing the construction of a derivation to be guided by the form of the goal sequent.

Such a sequent-based approach to process verification was proposed independently by Dam [4] and the second author [16], as a way of uniformly accounting for many specialist techniques for compositional reasoning that had appeared in the earlier literature, especially [17]. The approach has since been further developed in a series of papers by Dam and his co-workers [5]–[10]. We now discuss this previous research in more detail.

In [16], the second author introduced a sequent calculus for establishing properties expressed in Hennessy-Milner logic [11] (which is the recursion-free fragment of the modal μ-calculus). The main idea was to introduce a second form of assertion into sequents: transition assertions $p \xrightarrow{a} q$ expressing that process p evolves to process q under action a. Such assertions yield natural proof rules for modalities, and allow process operators $f(x_1, \ldots, x_n)$ to be incorporated into the proof system using proof rules reflecting their operational semantics. The approach is very general, and applies to any process calculus with an operational semantics in the GSOS format [1]. The main results of [16] were strong completeness results for the system. The proofs simultaneously established the admissibility of cut and hence the completeness of structural reasoning.

In [4]–[10], Dam and his co-workers have addressed the interesting question of how best to incorporate fixed-point reasoning into such sequent-based proof systems. The main difficulty is to provide methods that correctly interact with the cut rule, which, as described above, is essential for compositional reasoning. The difficulty it causes is due to the way cut requires the same formula to appear both on the left and right of sequents in separate branches of the proof, see [5]. In their more recent research, see, in particular, [9], Dam and Gurov have proposed dealing with this difficulty by extending the μ-calculus with a syntax for so-called explicit approximants. Specifically, the syntax is extended by including ordinal variables κ, which are semantically interpreted as ordinals, and by introducing formulae $\mu^{\kappa} X.\, \varphi$ and $\nu^{\kappa} X.\, \varphi$ standing for the κ-th iterations in the chain of approximations to the fixed-points $\mu X.\, \varphi$ and $\nu X.\, \varphi$ respectively. This machinery allows a sound notion of proof to be defined, by identifying certain repeats (up to substitution) of sequents in a derivation tree and by imposing a global "discharge" condition on a derivation tree, formulated in terms of ordinal variables. Over the course of their research, Dam, Gurov *et al* have: proved the completeness of their techniques for establishing properties of finite-state processes [5]; established completeness for sequents of the form $\vdash x : \varphi$, i.e. completeness with respect to μ-calculus validity [9]; and applied their techniques to such diverse languages as CCS [5, 8], the π-calculus [6] and Erlang [7, 10].

[1] In this paper, we write all inference rules and derivations in tableau form, i.e. with the goal (conclusion) on top and the subgoals (premises) underneath.

Overview

As the first contribution of the present paper, we provide a new proof system for incorporating fixed-point reasoning into the sequent-calculus approach. Our system is strongly based on Dam and Gurov's idea of using explicit fixed-point approximants. However, we provide an alternative formulation of these, not requiring ordinal variables. Instead, we use ordinary propositional variables X to range over approximants. To properly deal with these, we include an extra component on the left of sequents, a context D of approximant declarations. Such declarations have one of two forms: $X \leqslant \varphi$, which declares X to be an approximant of $\mu X.\,\varphi$; and $X \geqslant \varphi$, which declares X to be an approximant of $\nu X.\,\varphi$, see Section 2. Thus far, our approach can be seen as merely a (less expressive) reformulation of Dam and Gurov's syntax. However, we also extend the syntax of the μ-calculus in two significant ways. First, we allow explicit approximant declarations in formulae, introducing two new formula constructions: $\langle X \leqslant \varphi \rangle\, \psi$, which says that there exists an approximant X of $\mu X.\,\varphi$ such that ψ; and $[X \geqslant \varphi\,]\,\psi$, which says that ψ holds for all approximants X of $\nu X.\,\varphi$. In terms of expressivity, this is a harmless extension of the μ-calculus, as one can equivalently read the above as "letrec" expressions. For example, $\langle X \leqslant \varphi \rangle\, \psi$ can be understood as "letrec $X =_\mu \varphi$ in ψ" or, in other words, as $\psi[\,\mu X.\,\varphi\,/\,X]$. Nonetheless, explicit approximant declarations are useful for reasoning. Second, we incorporate a mechanism for approximant "modification" in formulae. If X is an approximant for $\mu X.\,\varphi$ then the formula $\langle -X \rangle\, \psi$ expresses that there exists another approximant X' of $\mu X.\,\varphi$ with $X' \subset X$ (proper inclusion) such that $\psi[\,X'\,/\,X]$. Dually, if X is an approximant for $\nu X.\,\varphi$ then $[+X\,]\,\psi$ expresses that, for all approximants X' of $\mu X.\,\varphi$ with $X' \supset X$ (proper containment), it holds that $\psi[\,X'\,/\,X]$.

The full proof system is presented in Section 3. The use of approximant variables and modifiers allows a straightforward definition of a global combinatorial condition for a derivation tree being a proof. The soundness of the proof system is then established as Theorem 1.

As already stated, one cannot hope for a general completeness result for the proof system. Indeed, if the proof system is complete for a class of processes then the property-checking problem is necessarily decidable for that class of processes, as one can use the proof system to recursively enumerate both the relation $p \models \varphi$ and its complement $p \models \neg\varphi$. Thus the best one can hope for is to establish restricted completeness results for classes of processes whose verification problem is decidable. One such widely considered class of processes is that of context-free processes, see e.g. [2]. The decidability of the property-checking problem for context-free processes is a direct consequence of the work of Muller and Schupp, who established the more general result that full monadic second-order logic (MSOL) is decidable over the wider class of pushdown transition graphs [14]. The decision problem for MSOL is known to be of non-elementary complexity. However, for the special case of μ-calculus properties, it is possible to obtain elementary decision algorithms [19, 3]. Also, Hungar and Steffen showed how alternation-free μ-calculus properties of context-free processes can be established by a tableau-style proof system embodying a form of compositional reasoning [12].

As the main contribution of this paper, we prove, in Section 4, that our general purpose proof system is complete for establishing arbitrary μ-calculus properties of context-free processes (Theorem 2). The proof builds on the techniques of Hungar and Steffen [12], but adapts them to the full μ-calculus, making essential use of explicit ν-approximant declarations, $[X \geqslant \varphi\,]\,\psi$, and modifiers, $[+X\,]\,\varphi$.

2 Modal μ-calculus and explicit approximants

Our treatment of the μ-calculus will be brief. The reader is referred to [18] for further details. We consider the μ-calculus in positive normal form, with formulae defined by the grammar:

$$\varphi \;::=\; X \mid \mathtt{ff} \mid \mathtt{tt} \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \langle a \rangle \varphi \mid [a]\varphi \mid \mu X.\,\varphi \mid \nu X.\,\varphi.$$

Here a ranges over a given set A of action symbols. Free and bound variables are defined as usual, and we identify formulae up to renaming of bound variables. We write $FV(\varphi)$ for the set of free

variables of φ, and we say that φ is *closed* if $FV(\varphi) = \emptyset$. The negation of a closed formula can be defined by induction on its structure using De Morgan duals.

Formulae are interpreted relative to a transition system $(T, \{\xrightarrow{a}\}_{a \in A})$ (here T is a set of states and each $\xrightarrow{a}$ is a binary relation on T). A formula φ is interpreted relative to an *environment* V mapping $FV(\varphi)$ to subsets of T, with its interpretation $\| \varphi \|_V \subseteq T$ defined as in [18].

Next we introduce approximants. Often this is done using ordinal indices. However, it is not strictly necessary to invoke such set-theoretic machinery. To emphasise this, we give a direct definition, which is interpretable in monadic third-order logic.

Definition 2.1 (μ-approximants). For any least-fixed-point formula $\mu X.\, \varphi$, its family of approximants $\mathcal{A}_V^{\mu X.\, \varphi}$, relative to an environment V defined on $FV(\mu X.\, \varphi)$, is the smallest family of subsets of T satisfying:

1. if $\mathcal{A}' \subseteq \mathcal{A}_V^{\mu X.\, \varphi}$ then $\bigcup \mathcal{A}' \in \mathcal{A}_V^{\mu X.\, \varphi}$, and
2. if $S \in \mathcal{A}_V^{\mu X.\, \varphi}$ then $\| \varphi \|_{V[S\,/\,X]} \in \mathcal{A}_V^{\mu X.\, \varphi}$.

Definition 2.2 (ν-approximants). For any greatest-fixed-point formula $\nu X.\, \varphi$, its family of approximants $\mathcal{A}_V^{\nu X.\, \varphi}$ relative to V is the smallest family of subsets of T satisfying:

1. if $\mathcal{A}' \subseteq \mathcal{A}_V^{\nu X.\, \varphi}$ then $\bigcap \mathcal{A}' \in \mathcal{A}_V^{\nu X.\, \varphi}$, and
2. if $S \in \mathcal{A}_V^{\nu X.\, \varphi}$ then $\| \varphi \|_{V[S\,/\,X]} \in \mathcal{A}_V^{\nu X.\, \varphi}$.

Note that, by taking $\mathcal{A}' = \emptyset$ we have that $\emptyset \in \mathcal{A}_V^{\mu X.\, \varphi}$, and $T \in \mathcal{A}_V^{\nu X.\, \varphi}$ (because $T = \bigcap \emptyset$ when $\emptyset$ is considered as the empty family of subsets of T).

Proposition 2.3.

1. $\| \mu X.\, \varphi \|_V = \bigcup \mathcal{A}_V^{\mu X.\, \varphi} \in \mathcal{A}_V^{\mu X.\, \varphi}$.
2. *If* $S \in \mathcal{A}_V^{\mu X.\, \varphi}$ *then* $S \subseteq \| \varphi \|_{V[S\,/\,X]}$.
3. *If* $S \in \mathcal{A}_V^{\mu X.\, \varphi}$ *then* $S = \bigcup \{ \| \varphi \|_{X[S'\,/\,X]} \mid S' \subset S \text{ and } S' \in \mathcal{A}_V^{\mu X.\, \varphi} \}$.
4. *There is no sequence* (S_i) *of elements of* $\mathcal{A}_V^{\mu X.\, \varphi}$ *such that* $S_0 \supset S_1 \supset S_2 \supset \ldots$.

Proposition 2.4.

1. $\| \nu X.\, \varphi \|_V = \bigcap \mathcal{A}_V^{\nu X.\, \varphi} \in \mathcal{A}_V^{\nu X.\, \varphi}$.
2. *If* $S \in \mathcal{A}_V^{\nu X.\, \varphi}$ *then* $S \supseteq \| \varphi \|_{V[S\,/\,X]}$.
3. *If* $S \in \mathcal{A}_V^{\nu X.\, \varphi}$ *then* $S = \bigcap \{ \| \varphi \|_{X[S'\,/\,X]} \mid S' \supset S \text{ and } S' \in \mathcal{A}_V^{\nu X.\, \varphi} \}$.
4. *There is no sequence* (S_i) *of elements of* $\mathcal{A}_V^{\nu X.\, \varphi}$ *such that* $S_0 \subset S_1 \subset S_2 \subset \ldots$.

As discussed in the introduction, the proof system will use a class of *extended formulae* containing declarations and modifiers for approximant variables:

$$\Phi \ ::= \ \varphi \ \mid \ \langle X \leqslant \varphi \rangle\, \Phi \ \mid \ [X \geqslant \varphi\,]\, \Phi \ \mid \ \langle -X \rangle\, \Phi \ \mid \ [+X\,]\, \Phi$$

In this definition, and henceforth, we use lower case Greek letters $\varphi, \psi, \ldots$ to range over ordinary μ-calculus formulae, and upper case letters $\Phi, \Psi, \ldots$ to range over extended formulae.

The sets of free variables of extended formulae are defined by:

$$\begin{array}{lcllcl} FV(\langle X \leqslant \varphi \rangle\, \Phi) & = & FV([X \geqslant \varphi\,]\, \Phi) & = & (FV(\varphi) \cup FV(\Phi)) \backslash \{X\} \\ FV(\langle -X \rangle\, \Phi) & = & FV([+X\,]\, \Phi) & = & FV(\Phi) \cup \{X\} \end{array}$$

Extended formulae are again identified up to renaming of bound variables.

The semantic interpretation of extended formulae is given relative to a finite set, D, of approximant *declarations*, each of the form $X \leqslant \varphi$ or $X \geqslant \varphi$. The former is a *μ-approximant* declaration, the latter a *ν-approximant* declaration, and in each case the *declared variable* is X. We write $DV(\mathsf{D})$ for the set of all variables declared in D.

The *declaration contexts* are produced as follows: (i) the empty set is a declaration context; (ii) if D is a declaration context, X is a variable not declared in D, and φ is a μ-calculus formula with $FV(\varphi) \subseteq DV(\mathsf{D}) \cup \{X\}$ then $\mathsf{D}, X \leqslant \varphi$ and $\mathsf{D}, X \geqslant \varphi$ are both declaration contexts (where we write comma for union). The set of *used variables* in a declaration context is defined by:

$$\begin{array}{lcl} UV(X \leqslant \varphi) & = & UV(X \geqslant \varphi) \;=\; FV(\varphi) \backslash \{X\} \\ UV(\mathsf{D}) & = & \bigcup \{\, UV(\delta) \mid \delta \in \mathsf{D} \,\} \end{array}$$

We next define the notion of an extended formula Φ being *well-formed* relative to a declaration context D. First, any μ-calculus formula φ is well-formed relative to any declaration context D with $FV(\varphi) \subseteq DV(\mathsf{D})$. Second, the extended formula $\langle X \leqslant \varphi \rangle\, \Phi$ (respectively $[\, X \geqslant \varphi \,]\, \Phi$) is well-formed relative to D if D,$X \leqslant \varphi$ (respectively D,$X \geqslant \varphi$) is a declaration context, where $X \notin DV(\mathsf{D})$ (which can be always assumed, by the identification of formulae up to renaming of bound variables), and Φ is well-formed relative to it. Finally, the extended formula $\langle -X \rangle\, \Phi$ (respectively $[\, +X \,]\, \Phi$) is well-formed relative to D if D contains a declaration $X \leqslant \varphi$ (respectively $X \geqslant \varphi$) and also $X \notin UV(\mathsf{D})$. By this definition, we have that $FV(\Phi) \subseteq DV(\mathsf{D})$ whenever Φ is well-formed relative to D.

Given a declaration context D, a D-*environment* is a function V mapping $DV(\mathsf{D})$ to subsets of T such that: for each declaration $X \leqslant \varphi$ in D, it holds that $V(X) \in \mathcal{A}_V^{\mu X.\, \varphi}$, and, for each declaration $X \geqslant \varphi$ in D, it holds that $V(X) \in \mathcal{A}_V^{\nu X.\, \varphi}$. To give a semantics to extended formulae, we define subsets $\| \Phi \|_V^{\mathsf{D}} \subseteq T$ whenever D is a declaration context, Φ is well-formed relative to D, and V is a D-environment.

$$\begin{array}{rcl} \| \varphi \|_V^{\mathsf{D}} & = & \| \varphi \|_V \\ \| \langle X \leqslant \varphi \rangle\, \Phi \|_V^{\mathsf{D}} & = & \bigcup \{ \| \Phi \|_{V[\,S\,/\,X\,]}^{\mathsf{D}, X \leqslant \varphi} \mid S \in \mathcal{A}_V^{\mu X.\, \varphi} \} \quad \text{where } X \notin DV(\mathsf{D}) \\ \| [\, X \geqslant \varphi \,]\, \Phi \|_V^{\mathsf{D}} & = & \bigcap \{ \| \Phi \|_{V[\,S\,/\,X\,]}^{\mathsf{D}, X \geqslant \varphi} \mid S \in \mathcal{A}_V^{\nu X.\, \varphi} \} \quad \text{where } X \notin DV(\mathsf{D}) \\ \| \langle -X \rangle\, \Phi \|_V^{\mathsf{D}} & = & \bigcup \{ \| \Phi \|_{V[\,S\,/\,X\,]}^{\mathsf{D}} \mid S \subset V(X) \text{ and } S \in \mathcal{A}_V^{\mu X.\, \varphi} \text{ where } X \leqslant \varphi \in \mathsf{D} \} \\ \| [\, +X \,]\, \Phi \|_V^{\mathsf{D}} & = & \bigcap \{ \| \Phi \|_{V[\,S\,/\,X\,]}^{\mathsf{D}} \mid S \supset V(X) \text{ and } S \in \mathcal{A}_V^{\nu X.\, \varphi} \text{ where } X \geqslant \varphi \in \mathsf{D} \} \end{array}$$

Note that the requirement that $X \notin UV(\mathsf{D})$ for $\langle -X \rangle\, \Phi$ to be well-formed relative to D ensures that $V[\,S\,/\,X\,]$ is indeed a D-context in the definition of $\| \langle -X \rangle\, \Phi \|_V^{\mathsf{D}}$ (and similarly for $[\, +X \,]\, \Phi$).

Proposition 2.5. *If V and V' are D-environments with $V(X) \subseteq V'(X)$ for all $X \in DV(\mathsf{D})$ then $\| \Phi \|_V^{\mathsf{D}} \subseteq \| \Phi \|_{V'}^{\mathsf{D}}$.*

Proposition 2.6.

1. $\| \langle X \leqslant \varphi \rangle\, \Phi \|_V^{\mathsf{D}} = \| \Phi \|_{V[\,\| \mu X.\, \varphi \|_V \,/\, X\,]}^{\mathsf{D}} = \| \Phi[\, \mu X.\, \varphi \,/\, X\,] \|_V^{\mathsf{D}}$.
2. $\| [\, X \geqslant \varphi \,]\, \Phi \|_V^{\mathsf{D}} = \| \Phi \|_{V[\,\| \nu X.\, \varphi \|_V \,/\, X\,]}^{\mathsf{D}} = \| \Phi[\, \nu X.\, \varphi \,/\, X\,] \|_V^{\mathsf{D}}$.
3. *If $X \leqslant \varphi \in \mathsf{D}$ then* $\| X \|_V^{\mathsf{D}} = \| \langle -X \rangle\, \varphi \|_V^{\mathsf{D}}$.
4. *If $X \geqslant \varphi \in \mathsf{D}$ then* $\| X \|_V^{\mathsf{D}} = \| [\, +X \,]\, \varphi \|_V^{\mathsf{D}}$.

3 The proof system

The proof system we present is general purpose in the sense that, following the approach of [16], it can be easily adapted to give a sound system for reasoning about any process algebra whose operational semantics is given in the GSOS format [1]. However, for brevity of exposition, we present proof rules for the special case of context-free processes only. We begin by reviewing the definition of such processes.

Definition 3.1 (Context-free system). A *context-free system* is specified by a finite set of *nonterminals* $\Sigma = \{\mathsf{P}_1, \ldots, \mathsf{P}_k\}$ together with a finite set $\mathcal{P}$ of *productions*, each of the form $\mathsf{P}_i \xrightarrow{a} \mathsf{p}$, where p ranges over Σ^* (the set of finite words over Σ) and a ranges over a finite set of action symbols A. The transition system $(T, \{\xrightarrow{a}_T\}_{a\in A})$ determined by the specification is defined as follows.

$$\begin{array}{rcl} T & = & \Sigma^* \\ \mathsf{s} \xrightarrow{a}_T \mathsf{t} & \text{iff} & \mathsf{s} = \mathsf{P}_i\,\mathsf{q} \text{ and } \mathsf{t} = \mathsf{p}\,\mathsf{q} \text{ for some production } \mathsf{P}_i \xrightarrow{a} \mathsf{p} \in \mathcal{P}. \end{array}$$

Here, as usual, a juxtaposition $\mathsf{p}\,\mathsf{q}$ means the concatenation of words p and q.

Example 3.2. As a running example, consider the system with a single nonterminal P, set of actions $A = \{a, b\}$, and with two productions: $\mathsf{P} \xrightarrow{a} \mathsf{PP}$ and $\mathsf{P} \xrightarrow{b} \varepsilon$, where ε is the empty word. This has as its transition system:

$$\varepsilon \underset{b}{\longleftarrow} \mathsf{P} \underset{b}{\overset{a}{\rightleftarrows}} \mathsf{P}^2 \underset{b}{\overset{a}{\rightleftarrows}} \mathsf{P}^3 \underset{b}{\overset{a}{\rightleftarrows}} \cdots$$

This is an infinite-state process in which no two distinct states are bisimilar to each other.

Henceforth in this section we assume that we have a fixed specification of a context-free system, as in Definition 3.1, and we write $(T, \{\xrightarrow{a}_T\}_{a\in A})$ for the transition system it determines.

The proof system uses process terms containing free process variables $x, y, \ldots$.

Definition 3.3 (Process term). A *process term* is a word of one of the following two forms: either $\mathsf{p}\,x$, where $\mathsf{p} \in \Sigma^*$ and x is a process variable; or p where $\mathsf{p} \in \Sigma^*$.

We use $p, q, \ldots$ to range over process terms. By a *process substitution* we shall mean a mapping θ from process variables to process terms. The substituted term $p\,[\,\theta\,]$ is defined in the obvious way. We write $\Gamma\,[\,\theta\,]$ for the set $\{\,p\,[\,\theta\,] : \Phi \mid p : \Phi \in \Gamma\}$.

The restriction of process variables to the rightmost position in a process term may seem unnatural. However, the above definition of process term is the one that derives from the simplest formulation of context-free systems in GSOS format. Under this formulation, one has a unary process operator for each nonterminal $\mathsf{P}_1, \ldots, \mathsf{P}_n$, and also a single process constant, ε. The productions of the system are then easily recast as GSOS operational rules.

Process terms are interpreted relative to *process environments* ρ mapping process variables to states in the transition system T. We extend ρ to a function (also called ρ) from process terms to T by: $\rho(\mathsf{p}\,x) = \mathsf{p}\,\rho(x)$ and $\rho(\mathsf{p}) = \mathsf{p}$.

Sequents will be built from two forms of assertion: *verification assertions* of the form $p : \Phi$, where Φ is an extended formula, as in Section 2; and *transition assertions* of the form $p \xrightarrow{a} q$. We use $J, K, \ldots$ to range over assertions. Given a declaration context D, as in Section 2, an assertion is a D-*assertion* if it is either a verification assertion $p : \Phi$ with Φ well-formed relative to D, or a transition assertion.

Definition 3.4 (Sequent). *Sequents* have the form $\mathsf{D}\,;\,\Gamma \vdash \Delta$ where: D is a declaration context and Γ and Δ are finite sets of D-assertions.

Semantically, assertions and sequents will always be interpreted relative to the transition system $(T, \{\xrightarrow{a}_T\}_{a\in A})$. Given a D-environment V and a process environment ρ, the relation $\models_{V\rho} J$, for D-assertions J, is defined by:

$$\begin{array}{rcl} \models_{V\rho} p : \Phi & \text{iff} & \rho(p) \in \| \Phi \|^{\mathsf{D}}_V \\ \models_{V\rho} p \xrightarrow{a} q & \text{iff} & \rho(p) \xrightarrow{a}_T \rho(q) \end{array}$$

We write $\mathsf{D}\,;\,\Gamma \models_{V\rho} \Delta$ to mean that if $\models_{V\rho} J$, for all $J \in \Gamma$, then there exists $K \in \Delta$ such that $\models_{V\rho} K$. We write $\mathsf{D}\,;\,\Gamma \models \Delta$ to mean that $\mathsf{D}\,;\,\Gamma \models_{V\rho} \Delta$ for all V and ρ.

The proof system will provide a sound means of establishing sequents $\mathsf{D}\,;\,\Gamma \vdash \Delta$ such that $\mathsf{D}\,;\,\Gamma \models \Delta$. The rules are presented in Figures 1 and 2. The rules in Figure 1 concern the modal fragment of the logic, and are essentially from [16]. For example, the operational rules are exactly the general GSOS rules of [16] when specialised to the case of context-free processes under their GSOS formulation referred to earlier. Figure 2 presents the crucial rules for fixed points and explicit approximations.

We emphasise again that we write the rules in tableau style with the *goal* sequent above the line and its (possibly empty) set of *subgoals* below the line. As is standard, we formulate the rules using comma for (not necessarily disjoint) union and omitting set delimiters from singleton sets. Rules are applicable only in instances that the subgoals produced are indeed sequents according to Definition 3.4. Certain rules have additional side conditions, written on the right. In particular, the "freshness" side conditions require that the identified variable does not already appear free in the goal above the line. In the rules ($\langle -X \rangle$) and ($[+X\,]$), we use the abbreviations:

$$\begin{aligned} \langle -X \rangle\,\Gamma &= \{\, p\!:\langle -X \rangle\,\Phi \mid p\!:\Phi \in \Gamma\}, \\ [+X\,]\,\Gamma &= \{\, p\!:[+X\,]\,\Phi \mid p\!:\Phi \in \Gamma\}. \end{aligned}$$

Next we formulate the condition for a derivation tree to be a proof. By a *leaf* in a derivation tree, we mean a sequent occurrence in the tree such that no rule has been applied with that sequent occurrence as goal (thus sequents to which a rule with an empty set of subgoals has been applied *do not* count as leaves, even though they have no child sequents).

Definition 3.5 (Repeat). In a derivation tree, a leaf $\mathsf{D}\,;\,\Gamma \vdash \Delta$ is a *repeat* of another sequent occurrence $\mathsf{D}'\,;\,\Gamma' \vdash \Delta'$ if $\mathsf{D}' \subseteq \mathsf{D}$ and there exists a process substitution θ such that $\Gamma'\,[\,\theta\,] \subseteq \Gamma$ and $\Delta'\,[\,\theta\,] \subseteq \Delta$.

Definition 3.6 (Pre-proof). A *pre-proof* is a derivation tree in which, to each leaf $\mathsf{D}\,;\,\Gamma \vdash \Delta$, there is an assigned sequent occurrence $\mathsf{D}'\,;\,\Gamma' \vdash \Delta'$ (the *companion* of the leaf) such that $\mathsf{D}\,;\,\Gamma \vdash \Delta$ is a repeat of $\mathsf{D}'\,;\,\Gamma' \vdash \Delta'$.

In the above definitions, it is worth noting that the companion is not required to appear on the branch from the root sequent to the leaf.

We shall consider a pre-proof as a directed graph whose vertices are sequent occurrences in the pre-proof, and with edges of two kinds: (i) edges from the goal of a rule application to each subgoal (if any) of the goal; (ii) an edge from each leaf to its companion. By a (finite or infinite) *path* through a pre-proof, we mean a sequence $(\mathcal{S}_i)_{0 \le i < n \le \infty}$ of sequent occurrences forming a directed path through the graph. We say that a rule is *applied along* a path $(\mathcal{S}_i)$ if the path contains two consecutive sequents $\mathcal{S}_i$ and $\mathcal{S}_{i+1}$ with $\mathcal{S}_i$ the goal of the rule and $\mathcal{S}_{i+1}$ one of its subgoals.

Definition 3.7 (Preservation). A path $(\mathcal{S}_i)$ *preserves* an approximant variable X if, for every sequent $\mathsf{D}\,;\,\Gamma \vdash \Delta$ occurring on the path, $X \in DV(\mathsf{D})$.

Definition 3.8 (Progress). A μ-approximant variable X *progresses* on a path $(\mathcal{S}_i)$ if it is preserved by the path and the rule ($\langle -X \rangle$) is applied along the path. Similarly, a ν-approximant variable X *progresses* if it is preserved and the rule ($[+X\,]$) is applied.

We say that X progresses *infinitely often* on an infinite path $(\mathcal{S}_i)_{i \ge 0}$ if, for all $n \in \mathbb{N}$, it holds that X progresses on the tail path $(\mathcal{S}_i)_{i \ge n}$.

Definition 3.9 (Proof). A pre-proof is a *proof* if, for every infinite path $(\mathcal{S}_i)_{i \ge 0}$ through it, there exist an approximant variable X and a tail $(\mathcal{S}_i)_{i \ge n}$ on which X progresses infinitely often.

We remark that this condition is necessarily global, in the sense that it cannot be reformulated as a condition to be satisfied by each repeat individually. However, we do at least have the result below, whose proof is given in Appendix A.

Proposition 3.10. *It is decidable whether a pre-proof is a proof or not.*

General rules

$$(\text{Axiom})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta}{}\ \Gamma \cap \Delta \neq \emptyset \qquad (\text{Weak})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta}{\mathsf{D}'\,;\,\Gamma' \vdash \Delta'}\ \mathsf{D}' \subseteq \mathsf{D},\ \Gamma' \subseteq \Gamma,\ \Delta' \subseteq \Delta$$

$$(\text{Cut})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ J \qquad \mathsf{D}\,;\,\Gamma,\ J \vdash \Delta} \qquad (\text{Sub})\ \frac{\mathsf{D}\,;\,\Gamma\,[\,\theta\,] \vdash \Delta\,[\,\theta\,]}{\mathsf{D}\,;\,\Gamma \vdash \Delta}$$

Logical rules

$$(\mathtt{ff}\text{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\mathtt{ff} \vdash \Delta}{} \qquad (\mathtt{tt}\text{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\mathtt{tt}}{}$$

$$(\vee\text{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\varphi_1 \vee \varphi_2 \vdash \Delta}{\mathsf{D}\,;\,\Gamma,\ p{:}\varphi_1 \vdash \Delta \qquad \mathsf{D}\,;\,\Gamma,\ p{:}\varphi_2 \vdash \Delta} \qquad (\vee\text{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\varphi_1 \vee \varphi_2}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\varphi_1,\ p{:}\varphi_2}$$

$$(\wedge\text{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\varphi_1 \wedge \varphi_2 \vdash \Delta}{\mathsf{D}\,;\,\Gamma,\ p{:}\varphi_1,\ p{:}\varphi_2 \vdash \Delta} \qquad (\wedge\text{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\varphi_1 \wedge \varphi_2}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\varphi_1 \qquad \mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\varphi_2}$$

Modal rules

$$(\langle a\rangle\text{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\langle a\rangle\varphi \vdash \Delta}{\mathsf{D}\,;\,\Gamma,\ p \xrightarrow{a} x,\ x{:}\varphi \vdash \Delta}\ x \text{ fresh} \qquad (\langle a\rangle\text{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\langle a\rangle\varphi}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p \xrightarrow{a} q \qquad \mathsf{D}\,;\,\Gamma \vdash \Delta,\ q{:}\varphi}$$

$$([a]\text{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}[a]\varphi \vdash \Delta}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p \xrightarrow{a} q \qquad \mathsf{D}\,;\,\Gamma,\ q{:}\varphi \vdash \Delta} \qquad ([a]\text{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}[a]\varphi}{\mathsf{D}\,;\,\Gamma,\ p \xrightarrow{a} x \vdash \Delta,\ x{:}\varphi}\ x \text{ fresh}$$

Operational rules

$$(\mathsf{P_i}\text{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ \mathsf{P_i}\,q \xrightarrow{a} x \vdash \Delta}{\{\,\mathsf{D}\,;\,\Gamma[\,\mathsf{p}\,q\,/\,x] \vdash \Delta[\,\mathsf{p}\,q\,/\,x]\,\}_{\mathsf{P_i} \xrightarrow{a} \mathsf{p} \in \mathcal{P}}}\ x \notin q \qquad (\mathsf{P_i}\text{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ \mathsf{P_i}\,q \xrightarrow{a} \mathsf{p}\,q}{}\ \mathsf{P_i} \xrightarrow{a} \mathsf{p} \in \mathcal{P}$$

$$(\varepsilon\text{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ \varepsilon \xrightarrow{a} x \vdash \Delta}{}$$

Figure 1: Basic rules

Fixed-point rules

$$(\mu\mathrm{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\,\mu X.\,\varphi \vdash \Delta}{\mathsf{D}\,;\,\Gamma,\ p{:}\,\langle X \leqslant \varphi\rangle\,\varphi \vdash \Delta} \qquad (\mu\mathrm{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,\mu X.\,\varphi}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,\langle X \leqslant \varphi\rangle\,\varphi}$$

$$(\leqslant\text{-}\mu\mathrm{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\,\langle X \leqslant \varphi\rangle\,\Phi \vdash \Delta}{\mathsf{D}\,;\,\Gamma,\ p{:}\,\Phi[\,\mu X.\,\varphi\,/\,X] \vdash \Delta} \qquad (\leqslant\text{-}\mu\mathrm{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,\langle X \leqslant \varphi\rangle\,\Phi}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,\Phi[\,\mu X.\,\varphi\,/\,X]}$$

$$(\nu\mathrm{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\,\nu X.\,\varphi \vdash \Delta}{\mathsf{D}\,;\,\Gamma,\ p{:}\,[X \geqslant \varphi\,]\,\varphi \vdash \Delta} \qquad (\nu\mathrm{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,\nu X.\,\varphi}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,[X \geqslant \varphi\,]\,\varphi}$$

$$(\geqslant\text{-}\nu\mathrm{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\,[X \geqslant \varphi\,]\,\Phi \vdash \Delta}{\mathsf{D}\,;\,\Gamma,\ p{:}\,\Phi[\,\nu X.\,\varphi\,/\,X] \vdash \Delta} \qquad (\geqslant\text{-}\nu\mathrm{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,[X \geqslant \varphi\,]\,\Phi}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,\Phi[\,\nu X.\,\varphi\,/\,X]}$$

Approximant rules

$$(\leqslant\text{-}X\mathrm{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\,\langle X \leqslant \varphi\rangle\,\Phi \vdash \Delta}{\mathsf{D},\ X \leqslant \varphi\,;\,\Gamma,\ p{:}\,\Phi \vdash \Delta}\ X \text{ fresh} \qquad (\leqslant\text{-}X\mathrm{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,\langle X \leqslant \varphi\rangle\,\Phi}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,\Phi}\ X \leqslant \varphi \in \mathsf{D}$$

$$(X_\mu\mathrm{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\,X \vdash \Delta}{\mathsf{D}\,;\,\Gamma,\ p{:}\,\langle -X\rangle\,\varphi \vdash \Delta}\ X \leqslant \varphi \in \mathsf{D} \qquad (X_\mu\mathrm{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,X}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,\langle -X\rangle\,\varphi}\ X \leqslant \varphi \in \mathsf{D}$$

$$(\langle -X\rangle)\ \frac{\mathsf{D}\,;\,\langle -X\rangle\,\Gamma,\ \Gamma' \vdash \langle -X\rangle\,\Delta,\ \Delta'}{\mathsf{D}\,;\,\Gamma,\ \Gamma' \vdash \Delta,\ \Delta'}\ \Gamma \neq \emptyset,\ X \notin UV(\mathsf{D}) \cup FV(\Gamma')$$

$$(\geqslant\text{-}X\mathrm{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\,[X \geqslant \varphi\,]\,\Phi \vdash \Delta}{\mathsf{D}\,;\,\Gamma,\ p{:}\,\Phi \vdash \Delta}\ X \geqslant \varphi \in \mathsf{D} \qquad (\geqslant\text{-}X\mathrm{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,[X \geqslant \varphi\,]\,\Phi}{\mathsf{D},\ X \geqslant \varphi\,;\,\Gamma \vdash \Delta,\ p{:}\,\Phi}\ X \text{ fresh}$$

$$(X_\nu\mathrm{L})\ \frac{\mathsf{D}\,;\,\Gamma,\ p{:}\,X \vdash \Delta}{\mathsf{D}\,;\,\Gamma,\ p{:}\,[+X\,]\,\varphi \vdash \Delta}\ X \geqslant \varphi \in \mathsf{D} \qquad (X_\nu\mathrm{R})\ \frac{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,X}{\mathsf{D}\,;\,\Gamma \vdash \Delta,\ p{:}\,[+X\,]\,\varphi}\ X \geqslant \varphi \in \mathsf{D}$$

$$([+X\,])\ \frac{\mathsf{D}\,;\,[+X\,]\,\Gamma,\ \Gamma' \vdash [+X\,]\,\Delta,\ \Delta'}{\mathsf{D}\,;\,\Gamma,\ \Gamma' \vdash \Delta,\ \Delta'}\ \Delta \neq \emptyset,\ X \notin UV(\mathsf{D}) \cup FV(\Delta')$$

Figure 2: Fixed-point and approximant rules

Some words are in order about alternative choices that might be made in the definition of proof. On the one hand, it would be possible to have a more liberal notion of repeat, by allowing substitutions of approximant variables as well as of process terms. However, such a relaxation of the definition of repeat both complicates the definition of proof and destroys our proof of Proposition 3.10 (although we believe the result still holds). Also, we do not know of any application of the more general notion of proof that arises. On the other hand, one could opt instead for a more restrictive notion of proof, defined in terms of local conditions on the derivation tree. The proposition below, whose proof is given in Appendix A, encapsulates one possible such definition.

Proposition 3.11. *Suppose we have a pre-proof in which each sequent is of the form* $\mathsf{D}\,;\,\Gamma \vdash \Delta$ *with* D *a sequence rather than a set. Then the following conditions together suffice for the pre-proof to be a proof.*

1. *Every edge in the pre-proof is from a sequent* $\mathsf{D}\,;\,\Gamma \vdash \Delta$ *to a sequent* $\mathsf{D}'\,;\,\Gamma' \vdash \Delta'$ *such that one of* D *and* D' *is a prefix of the other.*
2. *For every leaf, the companion appears along the unique path in the derivation tree from the root sequent to the leaf.*
3. *For every leaf, there exists an approximant variable that progresses along the unique path in the derivation tree from the companion to the leaf.*

We shall use this proposition in our proof of Theorem 2 below. Thus, interestingly, the restricted notion of proof implicit in the proposition is sufficient for context-free completeness to hold. Nevertheless, the general notion of proof of Definition 3.9 seems essential in the general application of the proof system towards establishing modularity goals of the form (1) of Section 1.

In Figure 3 we give an example proof in the system, showing that the process P, from Example 3.2, satisfies the property $\nu X.\,\mu Y.\,[a]X \wedge [b]Y$, stating that action a occurs infinitely often along any infinite path of a and b actions. We include all rule applications, except for instances of weakening (Weak). The identified repeats determine a pre-proof, which is easily seen to be a proof using Proposition 3.11, as X progresses for each repeat.

Theorem 1 (Soundness). *If the sequent* $\mathsf{D}\,;\,\Gamma \vdash \Delta$ *has a proof then* $\mathsf{D}\,;\,\Gamma \models \Delta$.

We end the section by outlining the soundness argument. We stress that the proof adapts easily to arbitrary GSOS-defined process algebras, as in [16].

Lemma 3.12. *Suppose that there is a pre-proof with* $\mathcal{S}_0 = \mathsf{D}_0\,;\Gamma_0 \vdash \Delta_0$ *as root sequent. Suppose also that we have a* D*-environment* V_0*, and process environment* ρ_0 *with* $\mathsf{D}_0\,;\,\Gamma_0 \not\models_{V_0\rho_0} \Delta_0$*. Then there exist infinite sequences* (V_i)*,* (ρ_i) *and* $(\mathcal{S}_i = \mathsf{D}_i\,;\,\Gamma_i \vdash \Delta_i)$*, such that all the following hold.*

1. $(\mathcal{S}_i)$ *is a path through the pre-proof.*
2. *For all* i*,* $\mathsf{D}_i\,;\,\Gamma_i \not\models_{V_i\rho_i} \Delta_i$.
3. *If a* μ*-approximant* X *is preserved by a subpath* $(\mathcal{S}_i)_{m\le i\le n}$ *then* $V_m(X) \supseteq V_n(X)$*, and if* X *progresses on the subpath then* $V_m(X) \supset V_n(X)$.
4. *If a* ν*-approximant* X *is preserved by a subpath* $(\mathcal{S}_i)_{m\le i\le n}$ *then* $V_m(X) \subseteq V_n(X)$*, and if* X *progresses on the subpath then* $V_m(X) \subset V_n(X)$.

The proof is given in Appendix A.

Proof of Theorem 1. Suppose, for contradiction, that there is a proof with root sequent $\mathsf{D}\,;\,\Gamma \vdash \Delta$ but that $\mathsf{D}\,;\,\Gamma \not\models \Delta$. Then there exist V and ρ such that $\mathsf{D}\,;\,\Gamma \not\models_{V\rho} \Delta$. Thus there is an infinite path through the proof satisfying properties 1–4 of Lemma 3.12. By the definition of proof, there is an approximant variable X that progresses infinitely often along some tail of this path. If X is a μ-approximant, then, by property 3 of the lemma, there is an infinite sequence $i_0 < i_1 < i_2 < \ldots$ with $V_{i_0}(X) \supset V_{i_1}(X) \supset V_{i_2}(X) \supset \ldots$. But this contradicts Proposition 2.3.4. Similarly, if X is a ν-approximant, then there exists an infinite sequence $V_{i_0}(X) \subset V_{i_1}(X) \subset V_{i_2}(X) \subset \ldots$ contradicting Proposition 2.4.4. So the assumption that $\mathsf{D}\,;\,\Gamma \not\models \Delta$ must have been incorrect. □

Abbreviations : $V \equiv \nu X.\, \mu Y.\, [a]X \wedge [b]Y$,
$U \equiv \mu Y.\, [a]X \wedge [b]Y$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \mathsf{P}:V}}{\vdash \varepsilon:[X\geqslant U\,]U}}{X\geqslant U\,;\ \vdash \varepsilon:U}}{X\geqslant U\,;\ \vdash \varepsilon:\langle Y\leqslant [a]X\wedge[b]Y\rangle\,[a]X\wedge[b]Y}}{X\geqslant U\,;\ \vdash \varepsilon:[a]X\wedge[b]U}}{X\geqslant U\,;\ \vdash \varepsilon:[a]X}}{X\geqslant U\,;\ \varepsilon\xrightarrow{a} x\ \vdash\ x:X}\qquad \dfrac{\dfrac{}{X\geqslant U\,;\ \vdash \varepsilon:[b]U}}{X\geqslant U\,;\ \varepsilon\xrightarrow{b} x\ \vdash\ x:U}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varepsilon:[X\geqslant U\,]U\ \vdash\ \mathsf{P}:V}}{x:[X\geqslant U\,]U\ \vdash\ \mathsf{P}\,x:V}}{x:[X\geqslant U\,]U\ \vdash\ \mathsf{P}\,x:[X\geqslant U\,]U}}{X\geqslant U\,;\ x:[X\geqslant U\,]U\ \vdash\ \mathsf{P}\,x:U}}{\vdots}\ (\mathrm{Sub})$$

We continue with the right-hand branch.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdots}}{X\geqslant U\,;\ x:U\ \vdash\ \mathsf{P}\,x:U}\ (\star)}{X\geqslant U\,;\ x:U\ \vdash\ \mathsf{P}\,x:\langle Y\leqslant [a]X\wedge[b]Y\rangle\,[a]X\wedge[b]Y}}{X\geqslant U\,;\ x:U\ \vdash\ \mathsf{P}\,x:[a]X\wedge[b]U}}{X\geqslant U\,;\ x:U\ \vdash\ \mathsf{P}\,x:[a]X}}{X\geqslant U\,;\ x:U,\ \mathsf{P}\,x\xrightarrow{a} y\ \vdash\ y:X}}{X\geqslant U\,;\ x:U\ \vdash\ \mathsf{PP}\,x:X}\qquad \dfrac{\dfrac{\dfrac{}{X\geqslant U\,;\ x:U\ \vdash\ \mathsf{P}\,x:[b]U}}{X\geqslant U\,;\ x:U,\ \mathsf{P}\,x\xrightarrow{b} y\ \vdash\ y:U}}{X\geqslant U\,;\ x:U\ \vdash\ x:U}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{X\geqslant U\,;\ x:U\ \vdash\ \mathsf{P}\,x:[+X\,]U}}{X\geqslant U\,;\ x:U\ \vdash\ \mathsf{P}\,x:U}}{X\geqslant U\,;\ \mathsf{P}\,x:[+X\,]U\ \vdash\ \mathsf{PP}\,x:X}}{X\geqslant U\,;\ \mathsf{P}\,x:[+X\,]U\ \vdash\ \mathsf{PP}\,x:[+X\,]U}}{X\geqslant U\,;\ \mathsf{P}\,x:U\ \vdash\ \mathsf{PP}\,x:U}$$

Both leaves are repeats of the sequent $(\star)$.

Figure 3: Example Proof

4 Completeness for context-free processes

Again in this section, we assume a fixed specification of a context-free system, as in Definition 3.1.

Theorem 2 (Context-free completeness). *For any $\mathsf{p}\in\Sigma^*$ and closed μ-calculus formula φ, if $\mathsf{p}\in\|\,\varphi\,\|$ then the sequent $\vdash \mathsf{p}:\varphi$ has a proof.*

The proof of completeness uses a variant of the property-checking games described in [18]. In a transition system $(T,\{\xrightarrow{a}_T\}_{a\in A})$, the property-checking game $\mathsf{G}(s,\varphi)$, where $s\in T$ and φ is a closed μ-calculus formula, is a game played by two players, Verifier and Refuter. Verifier aims to show that $s\in\|\,\varphi\,\|$ whereas Refuter attempts to refute this. We use an asymmetric variant of property-checking games, specifically designed to facilitate translating properties of games into the sequent calculus.

In this section, we shall assume representations of formulae in which all bound variables have different names, and that we only encounter fixed-point formulae $\mu X.\,\varphi$, $\nu X.\,\varphi$ with $X\in FV(\varphi)$.

For technical convenience, we use sequences, E, of greatest-fixed-point definitions called *ν-contexts*, together with their sets of *declared variables* $DV(\mathsf{E})$. These are defined by: (i) the empty sequence () is a ν-context with the empty set of declared variables; (ii) if E is a ν-context, $X\notin DV(\mathsf{E})$ and $FV(\varphi)\subseteq DV(E)\cup\{X\}$ then $\mathsf{E},\ X=\varphi$ is a ν-context with $DV(\mathsf{E})\cup\{X\}$ as its set

of declared variables. The equality $X = \varphi$ in a ν-context declares X to be the greatest fixed-point $\nu X.\, \varphi$. Part of the asymmetry in our games is that we do not use variables for μ-fixed-points.

Definition 4.1 (Position). A *position* is a triple (s, E, φ) where $s \in T$ is any state, E is a ν-context and φ is a formula such that $FV(\varphi) \subseteq DV(\mathsf{E})$ but, for all proper prefixes E' of E, $FV(\varphi) \not\subseteq \mathsf{E}'$.

Definition 4.2 (Move). The legitimate *moves* from one position (s, E, φ) to another are:

- If φ is $\mathtt{ff}$ then it is Verifier's move, but she is stuck.
- If φ is $\mathtt{tt}$ then it is Refuter's move, but he is stuck.
- If φ is $\psi_1 \vee \psi_2$ then Verifier chooses a disjunct ψ_j where $j \in \{1, 2\}$, and the next position is (s, E', ψ_j), where E' is the smallest prefix of E with $FV(\psi_j) \subseteq DV(\mathsf{E}')$.
- If φ is $\psi_1 \wedge \psi_2$ then Refuter chooses a conjunct ψ_j where $j \in \{1, 2\}$, and the next position is (s, E', ψ_j), where E' is the smallest prefix of E with $FV(\psi_j) \subseteq DV(\mathsf{E}')$.
- If φ is $\langle a \rangle \psi$ then Verifier chooses a transition $s \xrightarrow{a} t$, and the next position is (t, E, ψ).
- If φ is $[a]\psi$ then Refuter chooses a transition $s \xrightarrow{a} t$, and the next position is (t, E, ψ).
- If φ is $\mu X.\, \psi$ then it is (arbitrarily) Verifier's move and the next position is $(s, \mathsf{E}, \psi[\, \mu X.\, \psi \,/\, X])$.
- If φ is $\nu X.\, \psi$ then it is (arbitrarily) Refuter's move and the next position is (s, E', ψ) where E' is $\mathsf{E},\ X = \psi$.
- If φ is X where $X = \psi \in \mathsf{E}$ then it is (arbitrarily) Refuter's move and the next position is (s, E, ψ).

Definition 4.3 (Play). A *play* is a finite or infinite sequence $(s_i, \mathsf{E}_i, \varphi_i)_i$ of positions where each position $(s_{k+1}, \mathsf{E}_{k+1}, \varphi_{k+1})$ is produced from $(s_k, \mathsf{E}_k, \varphi_k)$ by following one of the moves above.

The next three definitions should be compared to Definitions 3.7–3.9.

Definition 4.4 (Preservation). We say that a play $(s_i, \mathsf{E}_i, \varphi_i)_i$ *preserves* a variable X if, for each E_i in the play, $X \in DV(\mathsf{E}_i)$.

Definition 4.5 (Progress). We say that a fixed-point variable X *progresses* along a play if it is preserved by the play and the play contains a move away from a position (s, E, X).

Definition 4.6 (Winning play). The Verifier *wins* a play either if the play is finite and its last position is one at which it is Refuter's move, or if the play is infinite and there exist a variable X and a tail of the play such that X progresses infinitely often along the tail.

Definition 4.7 (The game $\mathsf{G}(s, \varphi)$). The *game* $\mathsf{G}(s, \varphi)$, where φ is a closed formula, is played on the set of all positions reachable from the *initial position* $(s,\ (),\ \varphi)$. The game is a two player game, played by Verifier and Refuter, with play starting from the initial position.

For ordinary property-checking games, the following result appears in [18, §6.3]. The adaptation to our games is straightforward.

Proposition 4.8. *If $s \in \| \varphi \|$ then Verifier has a history-free winning strategy for $\mathsf{G}(s, \varphi)$.*

We now begin the proof of Theorem 2. Henceforth, suppose that $\mathsf{p}_0 \in \Sigma^*$ is such that $\mathsf{p}_0 \in \| \varphi_0 \|$. We use the game $\mathsf{G}(\mathsf{p}_0, \varphi_0)$ to construct a proof of the sequent $\vdash \mathsf{p}_0 : \varphi_0$.

Henceforth, all plays will be of the game $\mathsf{G}(p_0, \varphi_0)$. By Proposition 4.8, Verifier has a history-free winning strategy for this game. We henceforth fix on one such strategy, and we call a play a *V-play* if all Verifier's moves in the play follow the strategy. We write $\mathbf{u}_0$ for the initial position

$(\mathsf{p}_0, (), \varphi_0)$, From now on, we shall only consider those positions that arise in some V-play from $\mathbf{u}_0$. We use $\mathbf{u}, \mathbf{v}, \mathbf{w}, \ldots$ to range over such positions, and $\pi, \tau \ldots$ to range over V-plays starting from any such position. Note that Verifier wins any infinite V-play. We write $\mathbf{u}\pi$ and $\pi\mathbf{v}$ to mean that $\mathbf{u}$ and $\mathbf{v}$ are the first and last positions in π respectively. Given two V-plays $\pi_1\mathbf{v}$ and $\mathbf{v}\pi_2$, we write $\pi_1\pi_2$ for the evident concatenation of the two plays.

To assist the reader, before plunging into details, we give a brief summary the proof structure. We consider sequents of the restricted form:

$$\mathsf{D}\,;\, x{:}\,\Psi_1,\ \ldots,\ x{:}\,\Psi_k \vdash \mathsf{P}\,x{:}\,\varphi \tag{2}$$

where P is any nonterminal. Each such sequent is constructed with reference to a position of the form $\mathbf{u} = (\mathsf{P}\,\mathsf{q}, \mathsf{E}, \varphi)$, with each assumption $x{:}\,\Psi_i$ being determined by a V-play π from $\mathbf{u}$ to some position $\mathbf{v}$ whose state is q. Importantly, the extended formula Ψ_i contains approximant declarations and modifiers that reflect preservation and progress properties of the play π. We use Verifier's strategy to construct a derivation tree in which individual rule applications can be combined into larger steps between sequents of the form (2). Crucially, only finitely many distinct such sequents occur in the constructed derivation, enabling the derivation tree to terminate in repeats. Moreover, the resulting pre-proof is a proof because the required preservation and progress properties of paths through the proof follow from the analogous properties of winning V-plays.

Now, for the details. Given a play π ending in the position (s, E, φ), we define functions $\mathit{regen}_\pi(\mathsf{E}',\, \Phi)$ and $\mathit{prog}_\pi(\mathsf{E}',\, \Phi)$ for prefixes E' of E and extended formulae Φ with $FV(\Phi) \subseteq DV(\mathsf{E}')$. These are defined by:

$$\mathit{prog}_\pi(\mathsf{E}',\, \Phi) \quad = \quad \begin{cases} \mathit{regen}_\pi(\mathsf{E}',\, [{+}X\,]\,\Phi) & \text{if } \mathsf{E}' \text{ is } \mathsf{E}'', X{=}\varphi \text{ and } X \text{ progresses on a tail of } \pi \\ \mathit{regen}_\pi(\mathsf{E}',\, \Phi) & \text{otherwise} \end{cases}$$

$$\mathit{regen}_\pi(\mathsf{E}',\, \Phi) \quad = \quad \begin{cases} \mathit{prog}_\pi(\mathsf{E}'',\, [X \geqslant \varphi\,]\,\Phi) & \text{if } \mathsf{E}' \text{ is } \mathsf{E}'', X{=}\varphi \text{ and } \pi \text{ does not preserve } X \\ \Phi & \text{otherwise} \end{cases}$$

Definition 4.9 (Characteristic Formula). For any play π ending in (s, E, φ), its *characteristic formula* $\chi(\pi)$ is $\mathit{prog}_\pi(\mathsf{E},\, \varphi)$.

Definition 4.10 (Assumption set). For any position $\mathbf{u} = (\mathsf{p}, \mathsf{E}, \varphi)$, its *assumption set* relative to q is the set:

$$\mathit{AS}(\mathbf{u}, \mathsf{q}) \quad = \quad \{\chi(\pi) \mid \mathbf{u}\pi\mathbf{v} \text{ is a V-play with } \mathbf{v} = (\mathsf{q}, \mathsf{E}', \psi)\}.$$

Definition 4.11 (Canonical sequent). For any position $\mathbf{u} = (\mathsf{p}\,\mathsf{q}, \mathsf{E}, \varphi)$ the *canonical sequent* relative to p is the sequent

$$\mathcal{S}(\mathbf{u}, \mathsf{p}) \quad = \quad \mathsf{D}_\mathsf{E}\,;\, \{x{:}\,\Psi \mid \Psi \in \mathit{AS}(\mathbf{u}, \mathsf{q})\} \vdash \mathsf{p}\,x{:}\,\varphi, \tag{3}$$

where $\mathsf{D}_\mathsf{E} = \{X \geqslant \psi \mid X{=}\psi \text{ occurs in } \mathsf{E}\}$.

To justify this definition, we need to show that the set $\mathit{AS}(\mathbf{u}, \mathsf{q})$ is finite. This follows from:

Lemma 4.12 (Finiteness).

1. *Only finitely many different formulae φ occur in positions in $\mathsf{G}(\mathsf{p}_0, \varphi_0)$.*
2. *Only finitely many ν-contexts E occur in positions in $\mathsf{G}(\mathsf{p}_0, \varphi_0)$.*
3. *The set $\{\chi(\pi) \mid \pi$ is any play$\}$ is finite.*

Lemma 4.13 (Main lemma). *For any position $\mathbf{u} = (\mathsf{p}\,\mathsf{q}, \mathsf{E}, \varphi)$ the canonical sequent $\mathcal{S}(\mathbf{u}, \mathsf{p})$ has a proof.*

The proof combines a couple of sublemmas, whose proofs are deferred to Appendix B. Importantly, all the derivation trees referred to conform to property 1 of Proposition 3.11, where the sequence ordering on declaration contexts arises from their origin as ν-contexts.

Lemma 4.14. *Given a position* $\mathbf{u} = (\mathsf{Q}_1 \dots \mathsf{Q}_k\, \mathsf{r}, \mathsf{E}, \varphi)$*, where* $\mathsf{Q}_1, \dots, \mathsf{Q}_k$ *are nonterminals, the sequent* $\mathcal{S}(\mathbf{u}, \mathsf{Q}_1 \dots \mathsf{Q}_k)$ *occurs as the root of a derivation tree in which each leaf has the form* $\mathcal{S}_\pi = \mathcal{S}(\mathbf{v}_\pi, \mathsf{Q}_i)$ *where* $\mathbf{u}\pi\mathbf{v}_\pi$ *is a V-play and* $\mathbf{v}_\pi = (\mathsf{Q}_i \dots \mathsf{Q}_k\, \mathsf{r}, \mathsf{E}_\pi, \psi_\pi)$ *for some* i*. Moreover, if the play* π *preserves (respectively progresses on)* X *then so does the unique path from the root to* $\mathcal{S}_\pi$*.*

Lemma 4.15. *Given a position* $\mathbf{u} = (\mathsf{Q}\, \mathsf{r}, \mathsf{E}, \varphi)$*, where* Q *is nonterminal, the sequent* $\mathcal{S}(\mathbf{u}, \mathsf{Q})$ *occurs as the root of a derivation tree in which each leaf has the form* $\mathcal{S}_\pi = \mathcal{S}(\mathbf{v}_\pi, \mathsf{Q}_\pi)$*, where* Q_π *is nonterminal,* $\mathbf{v}_\pi = (\mathsf{Q}_\pi\, \mathsf{q}_\pi\, \mathsf{r}, \mathsf{E}_\pi, \psi_\pi)$ *and* $\mathbf{u}\pi\mathbf{v}_\pi$ *is a V-play containing at least one move. Moreover, if the play* π *preserves (respectively progresses on)* X *then so does the unique path to* $\mathcal{S}_\pi$ *in the derivation tree.*

Proof of Lemma 4.13. By Lemma 4.14, it suffices to build a proof for $\mathcal{S}(\mathbf{u}, \mathsf{Q})$ where Q is a nonterminal. We use Lemma 4.15 to construct a derivation tree in stages. At each stage, all leaves of the derivation will have the form $\mathcal{S}_\pi = \mathcal{S}(\mathbf{v}_\pi, \mathsf{Q}_\pi)$, where Q_π is nonterminal, $\mathbf{v}_\pi = (\mathsf{Q}_\pi\, \mathsf{q}, \mathsf{E}_\pi, \psi_\pi)$ and $\mathbf{u}\pi\mathbf{v}_\pi$ is a V-play. In such a derivation tree, a leaf $\mathcal{S}_\pi$ is marked as *successful* if $\pi = \pi'\tau$ where there is a sequent $\mathcal{S}_{\pi'}$ in the derivation (necessarily on the branch from the root to $\mathcal{S}_\pi$) such that: (i) $\mathcal{S}_\pi$ is a repeat of $\mathcal{S}_{\pi'}$; and (ii) some fixed-point variable X progresses on the V-play τ. If a leaf is unsuccessful then a new derivation tree is produced by applying Lemma 4.15 to the leaf (and appending the V-plays produced in Lemma 4.15 onto π). We first prove that this construction eventually produces a derivation tree in which every leaf is successful.

Suppose this is not the case. Then, by König's lemma, there exists a sequence of V-plays $\pi_0, \pi_1, \pi_2, \dots$ each with associated sequent $\mathcal{S}_{\pi_i}$ such that each π_i is a proper prefix of π_{i+1} and none of the sequent occurrences $\mathcal{S}_{\pi_i}$ is successful. Let π be the infinite V-play that the sequence (π_i) produces. Verifier wins this play, so $\pi = \pi'\tau$ where some fixed-point variable X progresses infinitely often along τ. As there are only finitely many nonterminals, by Lemma 4.12, only finitely many distinct sequents can occur as $\mathcal{S}_{\pi_i}$. Take some such sequent that occurs infinitely often. Then it must be the case that there exist $i < j$ such that: π' is a prefix of π_i, the sequents $\mathcal{S}_{\pi_i}$ and $\mathcal{S}_{\pi_j}$ are identical (thus the latter is a repeat of the former), and X progresses on τ'_j where $\pi_j = \pi_i\tau'_j$. Then $\mathcal{S}_{\pi_j}$ is successful, contradicting the assumption.

As every leaf is successful, the derivation tree is a pre-proof. We use Proposition 3.11 to show it is a proof. We have already mentioned that property 1 holds. Property 2 is immediate by (i) for successful sequents. Property 3 follows from (ii) and the progress claim of Lemma 4.15. □

Lemma 4.16. *For any position* $\mathbf{u} = (\mathsf{p}, \mathsf{E}, \varphi)$ *and* Ψ *in the assumption set* $AS(\mathbf{u}, \varepsilon)$ *the sequent* $\vdash \varepsilon : \Psi$ *has a proof.*

Again, see Appendix B for the proof.

Proof of Theorem 2. We must construct a proof for the sequent $\vdash \mathsf{p}_0 : \varphi_0$. We use (Cut) and Lemma 4.16 to reduce this to the goal $\{\varepsilon : \Psi \mid \Psi \in AS(\mathbf{u_0}, \varepsilon)\} \vdash \mathsf{p} : \varphi_0$. But this reduces by (Sub) to the sequent $\mathcal{S}(\mathbf{u_0}, \mathsf{p})$, which has a proof, by Lemma 4.13. □

5 Discussion and future work

Our proof of completeness for context-free processes makes essential use of approximant declarations and modifiers. These features can be incorporated into Dam and Gurov's proof system [9], by extending their syntax with ordinal quantifiers $\forall\kappa.\, \varphi$ and $\forall\kappa' < \kappa.\, \varphi$. Indeed, the completeness proof for context-free processes was originally developed in this context by the first author [15]. We do not know whether completeness holds for Dam and Gurov's system without ordinal quantifiers. Certainly, simple examples, such as that of Figure 3, are provable in their system, see [8].

It is natural to ask whether the approach in this paper might extend to obtain completeness for richer classes of processes, such as pushdown processes [14, 19, 3]. However, even the basic proof rules may have to be adapted for such processes, as they go beyond the process algebra idiom of being generated by bisimulation-preserving operators.

In a different direction, it would be very interesting to ascertain to what extent one can obtain completeness results for modularity goals of the form (1), see Section 1.

References

[1] B. Bloom, S. Istrail, and A.R. Meyer. Bisimulation can't be traced. *J. Assoc. Comput. Mach.*, 42:232–268, 1995.

[2] O. Burkart, D. Caucal, F. Moller, and B. Steffen. Verification over infinite states. In *Handbook of Process Algebra*, pages 545–623. Elsevier, 2001.

[3] O. Burkart and B. Steffen. Model checking the full modal mu-calculus for infinite sequential processes. *Theoretical Computer Science*, 221(1–2):251–270, 1999.

[4] M. Dam. Compositional proof systems for model checking infinite state processes. In *International Conference on Concurrency Theory*, pages 12–26, 1995.

[5] M. Dam. Proving properties of dynamic process networks. *Information and Computation*, 140(2):95–114, 1998.

[6] M. Dam. Proof systems for π-calculus logics. In R. de Queiroz, editor, *Logic for Concurrency and Synchronisation*. OUP, 2001.

[7] M. Dam, L. Fredlund, and D. Gurov. Toward parametric verification of open distributed systems. In A. Pnueli H. Langmaack and W.-P. de Roever, editors, *Compositionality: the Significant Difference*. Springer, 1998.

[8] M. Dam and D. Gurov. Compositional verification of CCS processes. In *Proceedings of PSI'99*, 1999.

[9] M. Dam and D. Gurov. μ-calculus with explicit points and approximations. *Journal of Logic and Computation*, to appear, 2001. Abstract in Proceedings of FICS 2000.

[10] L. Fredlund. A framework for reasoning about Erlang code. PhD Thesis, Swedish Institute of Computer Science, 2001.

[11] M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *J. Assoc. Comput. Mach.*, 32:137–161, 1985.

[12] H. Hungar and B. Steffen. Local model checking for context-free processes. *Nordic Journal of Computing*, 1(3):364–385, Fall 1994.

[13] D. Kozen. Results on the propositional μ-calculus. *Theoretical Computer Science*, 27:333–354, 1983.

[14] D.E. Muller and P.E. Schupp. The theory of ends, pushdown automata, and second-order logic. *Theoretical Computer Science*, 37:51–75, 1985.

[15] U. Schöpp. *Formal Verification of Processes*. MSc Dissertation, Division of Informatics, University of Edinburgh, 2001. Available as `http://www.dcs.ed.ac.uk/home/us/th.ps.gz`.

[16] A.K. Simpson. Compositionality via cut-elimination: Hennessy-Milner logic for an arbitrary GSOS. In *Logic in Computer Science*, pages 420–430, 1995.

[17] C.P. Stirling. Modal logics for communicating systems. *Theoretical Computer Science*, 49:311–347, 1987.

[18] C.P. Stirling. *Modal and Temporal Properties of Processes*. Texts in Computer Science. Springer, 2001.

[19] I. Walukiewicz. Pushdown Processes: Games and Model-Checking. *Information and Computation*, 164(2):234–263, January 2001.

Appendices

For refereeing purposes, we include appendices containing the proofs omitted from sections 3 and 4.

A Proofs from Section 3

Proof of Proposition 3.10. For each of the finitely many approximant variables X occurring in the pre-proof, mark a sequent $\mathsf{D}\,;\,\Gamma \vdash \Delta$ (i.e. a vertex of the graph) as *X-bad* if $X \notin DV(\mathsf{D})$ and as *X-good* if it is the goal sequent of a $(\langle -X \rangle)$ or $([+X])$ rule application. The property of being a proof equivalently says that, for every infinite directed path through the pre-proof graph (starting, without loss of generality, from the root sequent), there exists a process variable X such that the path is X-bad finitely often and X-good infinitely often. This is explicitly asking for a Rabin condition to hold along all infinite paths from the root, which is equivalent to the emptiness of the complement Rabin automaton. Thus the property is decidable. □

Rather than invoking such powerful machinery, it is, in fact, possible to give an explicit finitary combinatorial condition for a pre-proof to be a proof, along the lines of the discharge conditions in [9, 10, 15]. However, such conditions are necessarily phrased in terms of sets of leaves (and their companions), so the exponential blow-up of complementing a Rabin automaton is not avoided.

Proof of Proposition 3.11. Consider any infinite path $(\mathcal{S}_i)$ through the pre-proof. There are only finitely many sequent occurrences in the pre-proof, so, for some tail $(\mathcal{S}_i)_{i\geq n}$, every sequent in the tail occurs infinitely often in it. By property 1 of the proposition, there is some sequent $\mathcal{S}_j = \mathsf{D}_j\,;\,\Gamma_j \vdash \Delta_j$ in the tail such that D_j is a prefix of every declaration context appearing in the tail. As $\mathcal{S}_j$ occurs infinitely often in the tail, there is, by property 2, a leaf $\mathcal{S}_k$ in the tail and companion $\mathcal{S}_{k+1}$ such that $\mathcal{S}_j$ appears on the unique path in the derivation tree from $\mathcal{S}_{k+1}$ to $\mathcal{S}_k$. Let X be the approximant variable that, by property 3, progresses on this path. Then X is preserved by $(\mathcal{S}_i)_{i\geq n}$, because it is declared in D_j. Moreover, the rule by which X progresses is applied along every path in the pre-proof from $\mathcal{S}_{k+1}$ to $\mathcal{S}_k$. So, as these sequents occur infinitely often in the tail, X progresses infinitely often. □

Proof of Lemma 3.12. Suppose, for $k \geq 0$, we already have $(V_i)_{i\leq k}$, $(\rho_i)_{i\leq k}$ and $(\mathcal{S}_i)_{i\leq k}$ satisfying properties 1–4 of the Lemma. We construct V_{k+1}, ρ_{k+1} and $\mathcal{S}_{k+1}$.

If $\mathcal{S}_k$ is a leaf sequent then: define $\mathcal{S}_{k+1}$ $(= \mathsf{D}_{k+1}\,;\,\Gamma_{k+1} \vdash \Delta_{k+1})$ to be the companion of the leaf; define V_{k+1} to be the restriction of V_k to $DV(\mathsf{D}_{k+1})$; and define ρ_{k+1} to be the function $\rho \circ \theta$, where θ is some process substitution justifying the repeat. It is easily verified that properties 1–4 hold for the sequences $(V_i)_{i\leq k+1}$, $(\rho_i)_{i\leq k+1}$ and $(\mathcal{S}_i)_{i\leq k+1}$.

Otherwise, $\mathcal{S}_k$ is the goal in some rule application. Because of 1 above, we have to define $\mathcal{S}_{k+1}$ to be one of the subgoals of the rule. First, by 2, the rule cannot be an instance of (Axiom), (ffL), (ttR), $(P_i\mathrm{R})$ or $(\varepsilon\mathrm{L})$, as the goals of these rules are easily shown to be valid sequents. Thus the rule has at least one subgoal. To see which is selected and how V_{k+1} and ρ_{k+1} are defined, we proceed by case analysis on the rule applied. For brevity, we omit consideration of the rules in Figure 1, all of which are straightforward. Of the rules in Figure 2, we consider only the cases involving μ-fixed-points and μ-approximants. Dual arguments apply to the ν-fixed-point and ν-approximant rules.

In each case we show that property 2 holds for the selected $\mathcal{S}_{k+1}$ and that properties 3–4 hold of the sequences $(V_i)_{i\leq k+1}$ and $(\mathcal{S}_i)_{i\leq k+1}$.

(μL), (μR), ($\leqslant$-μL) or ($\leqslant$-μR) In each case define $\mathcal{S}_{k+1}$ to be the unique subgoal, and take $V_{k+1} = V_k$ and $\rho_{k+1} = \rho_k$. Property 2 holds by Proposition 2.6.1 together with the fixed-point identity $\| \mu X.\,\varphi \|_V = \| \varphi[\,\mu X.\,\varphi\,/\,X\,] \|_V$. Properties 3–4 hold trivially.

($\leqslant$-XL) Again, $\mathcal{S}_{k+1}$ is the unique subgoal and $\rho_{k+1} = \rho_k$. To define V_{k+1}, note that, because $\mathsf{D}_k\,;\,\Gamma_k \not\models_{V_k\rho_k} \Delta_k$, we have that $\rho_k(p) \in \| \langle X \leqslant \varphi \rangle\, \Phi \|_{V_k}^{\mathsf{D}_k}$ where $p\colon \langle X \leqslant \varphi \rangle\, \Phi \in \Gamma_k$ is the "active" assertion of the rule. So, by the definition of $\| \langle X \leqslant \varphi \rangle\, \Phi \|_{V_k}^{\mathsf{D}_k}$, there exists $S \in \mathcal{A}_{V_k}^{\mu X.\,\varphi}$

such that $\rho_k(p) \in \| \Phi \|^{\mathsf{D}_k, X \leqslant \varphi}_{V_k[\,S\,/\,X\,]}$. So defining $V_{k+1} = V_k[\,S\,/\,X\,]$, and 2 holds because X is fresh. Again 3–4 hold trivially.

($\leqslant$-$\boldsymbol{X}$R) $\mathcal{S}_{k+1}$ is the unique subgoal, $V_{k+1} = V_k$ and $\rho_{k+1} = \rho_k$. Because $\mathsf{D}_k\,;\,\Gamma_k \not\models_{V_k\rho_k} \Delta_k$, we have that $\rho_k(p) \notin \| \langle X \leqslant \varphi \rangle \Phi \|^{\mathsf{D}_k}_{V_k}$ where $p\colon \langle X \leqslant \varphi \rangle \Phi \in \Delta_k$ is the active assertion. So, by the definition of $\| \langle X \leqslant \varphi \rangle \Phi \|^{\mathsf{D}_k}_{V_k}$, for any $S \in \mathcal{A}^{\mu X.\,\varphi}_{V_k}$, it holds that $\rho_k(p) \notin \| \Phi[\,Z\,/\,X\,] \|^{\mathsf{D}_k, Z \leqslant \varphi[Z/X]}_{V_k[\,S\,/\,Z\,]}$, where $Z \notin DV(\mathsf{D})$. Thus, in particular, this holds for $S = V_k(X)$. But $\| \Phi[\,Z\,/\,X\,] \|^{\mathsf{D}_k, Z \leqslant \varphi[Z/X]}_{V_k[\,V_k(X)\,/\,Z\,]} = \| \Phi \|^{\mathsf{D}_k}_{V_k}$. So $\rho_k(p) \notin \| \Phi \|^{\mathsf{D}_k}_{V_k}$. Thus 2 holds. Again 3–4 hold trivially.

($\boldsymbol{X}_{\boldsymbol{\mu}}$L) or ($\boldsymbol{X}_{\boldsymbol{\mu}}$R) $\mathcal{S}_{k+1}$ is the unique subgoal, $V_{k+1} = V_k$ and $\rho_{k+1} = \rho_k$. Property 2 holds by Proposition 2.6.3. Properties 3–4 hold trivially.

($\langle -\boldsymbol{X} \rangle$) Again, $\mathcal{S}_{k+1}$ is the unique subgoal and $\rho_{k+1} = \rho_k$. We have that $\Gamma_k = \langle -X \rangle \Gamma,\ \Gamma'$ and $\Delta_k = \langle -X \rangle \Delta,\ \Delta'$ where, by the side condition on the rule, $\Gamma = \{p_1\colon \Phi_1, \ldots, p_l\colon \Phi_l\}$ is a non-empty set. Because $\mathsf{D}_k\,;\,\Gamma_k \not\models_{V_k\rho_k} \Delta_k$, we have that $\rho_k(p_j) \in \| \langle -X \rangle \Phi_j \|^{\mathsf{D}_k}_{V_k}$, for each $p_j\colon \Phi_j$ in Γ. So, by the definition of $\| \langle -X \rangle \Phi_j \|^{\mathsf{D}_k}_{V_k}$, we have, for each $p_j\colon \Phi_j$, that there exists $S_j \subset V(X)$ with $S_j \in \mathcal{A}^{\mu X.\,\varphi}_{V_k}$ (where $X \leqslant \varphi \in \mathsf{D}_k$) such that $\rho_k(p_j) \in \| \Phi_j \|^{\mathsf{D}_k}_{V_k[\,S_j\,/\,X\,]}$. Define $V_{k+1} = V_k[\,S_1 \cup \cdots \cup S_l\,/\,X\,]$. Then V_{k+1} is indeed a $\mathsf{D}_{k+1}(= \mathsf{D}_k)$-context because V_{k+1} agrees with V_k on all approximant variables other than $X \notin UV(\mathsf{D}_k)$ and $V_{k+1}(X) \in \mathcal{A}^{\mu X.\,\varphi}_{V_k} = \mathcal{A}^{\mu X.\,\varphi}_{V_{k+1}}$. Also, $V_{k+1}(X) \subset V_k(X)$, because Γ is non-empty. One now verifies: for each $p_j\colon \Phi_j \in \Gamma$, it holds that $\rho_{k+1}(p_j) \in \| \Phi_j \|^{\mathsf{D}_{k+1}}_{V_{k+1}}$, because $\| \Phi_j \|^{\mathsf{D}_k}_{V_k[\,S_j\,/\,X\,]} \subseteq \| \Phi_j \|^{\mathsf{D}_{k+1}}_{V_{k+1}}$ by Proposition 2.5; for all $p\colon \Phi \in \Gamma'$, it holds that $\rho_{k+1}(p) \in \| \Phi \|^{\mathsf{D}_{k+1}}_{V_{k+1}}$, because $X \notin FV(\Phi)$ so $\| \Phi \|^{\mathsf{D}_{k+1}}_{V_{k+1}} = \| \Phi \|^{\mathsf{D}_k}_{V_k}$; for all $p\colon \Phi \in \Delta$, it holds that $\rho_{k+1}(p) \notin \| \Phi \|^{\mathsf{D}_{k+1}}_{V_{k+1}}$, because $\rho_k(p) \notin \| \langle -X \rangle \Phi \|^{\mathsf{D}_k}_{V_k}$ and $V_{k+1}(X) \subset V_k(X)$; and, for all $p\colon \Phi \in \Delta'$, it holds that $\rho_{k+1}(p) \notin \| \Phi \|^{\mathsf{D}_{k+1}}_{V_{k+1}}$, again by Proposition 2.5 because $\| \Phi \|^{\mathsf{D}_{k+1}}_{V_{k+1}} \subseteq \| \Phi \|^{\mathsf{D}_k}_{V_k}$. Thus property 2 holds. Property 3 holds because, $V_{k+1}(X) \subset V_k(X)$. Property 4 holds trivially.

□

B Proofs from Section 4

We first state some facts about plays and characteristic formulae. The straightforward proofs are omitted.

For technical convenience, we use sequences Π called *prefix* of an extended formula. These are defined by (i) the empty sequence is a prefix of Φ; (ii) if Π is a prefix of Φ then $[X \geqslant \varphi\,]\,\Pi$ is a prefix of $[X \geqslant \varphi\,]\,\Phi$; (iii) if Π is a prefix of Φ then $[+X\,]\,\Pi$ is a prefix of $[+X\,]\,\Phi$. We write $\Pi\,\Phi$ to mean the formula that results from 'prefixing' the formula Φ with Π.

Lemma B.1. *For any position $\mathbf{u} = (s, \mathsf{E}, \varphi)$ and any play $\pi\mathbf{u}$ there exist ν-contexts E_1, E_2 and E_3 such that $\mathsf{E} = \mathsf{E}_1\mathsf{E}_2\mathsf{E}_3$ and E_2 consists of at most one definition and the following conditions hold: (i) $\mathsf{E}_1\mathsf{E}_2$ is a prefix of each context in π; (ii) any variable declared in E_1 is preserved by π but does not progress along π; (iii) any variable declared in E_2 progresses along π; (iv) any variable declared in E_3 is not preserved by π.*

Lemma B.2. *If $\mathbf{u} = (s, \mathsf{E}, \varphi)$ is a position in which E has the form E', $X = \varphi$ then $X \notin DV(\mathsf{D}_{\mathsf{E}'})$ and $X \notin UV(\mathsf{D}_{\mathsf{E}})$.*

Lemma B.3. *For all plays $\pi\mathbf{u}$ and $\mathbf{u}\tau$, there exist prefixes Π and Π' such that $\chi(\pi\tau) = \Pi\,\chi(\tau)$ and $\chi(\pi) = \Pi\,\Pi'\,\varphi$, where φ is the formula of $\mathbf{u}$.*

The next Lemma is used to obtain derivations in which each leaf is of the restricted form $\mathcal{S}(\mathbf{u}, \mathsf{p})$.

Lemma B.4. *Given positions* $\mathbf{u} = (\mathsf{p}\,\mathsf{r}, \mathsf{E}_\mathbf{u}, \varphi)$ *and* $\mathbf{v} = (\mathsf{q}\,\mathsf{r}, \mathsf{E}_\mathbf{v}, \psi)$ *and a V-play* $\mathbf{u}\pi\mathbf{v}$*, the following rule is derivable.*

$$\frac{\mathsf{D}_{\mathsf{E}_\mathbf{u}}\,;\,\{x\!:\!\Psi \mid \Psi \in \mathit{AS}(\mathbf{u},\mathsf{r})\} \vdash \mathsf{q}\,x\!:\!\chi(\pi) \qquad (A)}{\mathsf{D}_{\mathsf{E}_\mathbf{v}}\,;\,\{x\!:\!\Psi \mid \Psi \in \mathit{AS}(\mathbf{v},\mathsf{r})\} \vdash \mathsf{q}\,x\!:\!\psi \qquad (B)}$$

Note that (B) is $\mathcal{S}(\mathbf{v},\mathsf{q})$*. Furthermore, if the play* π *preserves (respectively progresses on)* X *then so does the unique path from* (A) *to* (B) *in the derivation tree.*

Proof. By definition, $\chi(\pi)$ has the form $\Pi\,\psi$, for some prefix Π. We will eliminate this prefix Π simultaneously with the prefixes on the left-hand side of the sequent using the following rules:

$$\frac{\mathsf{D}_\mathsf{E}\,;\,\Gamma \vdash [X \geqslant \varphi_X\,]\,\Phi}{\mathsf{D}_{\mathsf{E},X=\varphi_X}\,;\,\Gamma \cup \{x\!:\!\Psi \mid x\!:\![X \geqslant \varphi_X\,]\,\Psi \in \Gamma\} \vdash \Phi} \qquad \frac{\mathsf{D}_{\mathsf{E},X=\varphi_X}\,;\,\Gamma \vdash [{+}X\,]\,\Phi}{\mathsf{D}_{\mathsf{E},X=\varphi_X}\,;\,\Gamma \cup \{x\!:\!\Psi \mid x\!:\![{+}X\,]\,\Psi \in \Gamma\} \vdash \Phi}$$

where $\mathsf{E},\ X{=}\varphi_X$ is an arbitrary prefix of $\mathsf{E}_\mathbf{v}$. These two rules are derivable using ($\geqslant$-XR), ($\geqslant$-XL) and ($[{+}X\,]$), where the side-conditions for ($\geqslant$-XR) and ($[{+}X\,]$) are justified by Lemma B.2.

We start the derivation with the following weakening:

$$\frac{\mathsf{D}_{\mathsf{E}_\mathbf{u}}\,;\,\{x\!:\!\Psi \mid \Psi \in \mathit{AS}(\mathbf{u},\mathsf{r})\} \vdash \mathsf{q}\,x\!:\!\chi(\pi)}{\mathsf{D}_\mathsf{E}\,;\,\Gamma \vdash \mathsf{q}\,x\!:\!\chi(\pi)}$$

where $\Gamma = \{x\!:\!\Psi \mid \Psi \in \mathit{AS}(\mathbf{u},\mathsf{r})$ and $\Psi = \chi(\pi\tau)$ for some $\tau\}$, and E is the prefix of $\mathsf{E}_\mathbf{u}$ and $\mathsf{E}_\mathbf{v}$ consisting of declarations for exactly those variables that are preserved by π, which exists by Lemma B.1. The sequent in the subgoal is easily seen to be well formed.

We continue the derivation with the elimination of the prefix of $\chi(\pi)$ using the rules above. Let $\mathsf{E}_\mathbf{v} = \mathsf{E}\,\mathsf{E}'_\mathbf{v}$. By construction of E, we know that $\chi(\pi) = \mathit{prog}_\pi(\mathsf{E}_\mathbf{v}, \psi)$ is either $\mathit{prog}_\pi(\mathsf{E}'_\mathbf{v}, \psi)$ or $[{+}X\,]\,\mathit{prog}_\pi(\mathsf{E}'_\mathbf{v}, \psi)$. Furthermore, if $X{=}\varphi_X$, $\mathsf{E}''_\mathbf{v}$ is a tail of $\mathsf{E}'_\mathbf{v}$ then $\mathit{prog}_\pi(X{=}\varphi_X, \mathsf{E}''_\mathbf{v}, \psi)$ is either $[X \geqslant \varphi_X\,]\,\mathit{prog}_\pi(\mathsf{E}''_\mathbf{v}, \psi)$ or $[X \geqslant \varphi_X\,]\,[{+}X\,]\,\mathit{prog}_\pi(\mathsf{E}''_\mathbf{v}, \psi)$, since π does not preserve any variable in $\mathsf{E}'_\mathbf{v}$. This shows that after any number of applications of the two rules above, the declaration contexts have the form required in these rules. We can therefore apply these rules repeatedly to arrive at the sequent $\mathsf{D}_{\mathsf{E}\,\mathsf{E}'_\mathbf{v}}\,;\,\Gamma' \vdash \mathsf{q}\,x\!:\!\psi$, where

$$\Gamma' = \{x\!:\!\Psi \mid \text{there exist prefixes } \Pi \text{ and } \Pi' \text{ such that } x\!:\!\Pi\,\Psi \in \Gamma \text{ and } \chi(\pi) = \Pi\,\Pi'\,\psi\}.$$

We now show $\{x\!:\!\Psi \mid \Psi \in \mathit{AS}(\mathbf{v},\mathsf{r})\} \subseteq \Gamma'$. Each formula $\Psi \in \mathit{AS}(\mathbf{v},\mathsf{r})$ is $\chi(\tau)$ for some play $\mathbf{v}\tau\mathbf{w}$ where the state of $\mathbf{w}$ is r. Then, by definition, $\chi(\pi\tau)$ must be an element of $\mathit{AS}(\mathbf{u},\mathsf{r})$, hence $x\!:\!\chi(\pi\tau) \in \Gamma$. Lemma B.3 shows the existence of a prefixes Π and Π' such that $\chi(\pi\tau) = \Pi\,\chi(\tau)$ and $\chi(\pi) = \Pi\,\Pi'\,\varphi$. This implies $x\!:\!\chi(\tau) \in \Gamma'$, which completes the argument.

We can therefore apply the weakening rule to arrive at $\mathsf{D}_{\mathsf{E}_\mathbf{v}}\,;\,\{x\!:\!\Psi \mid \Psi \in \mathit{AS}(\mathbf{v},\mathsf{r})\} \vdash \mathsf{q}\,x\!:\!\psi$, which gives a derivation of the required form.

It remains to show the assertions about progress and preservation. In the construction above, the definition context of each sequent on the unique path from (A) to (B) contains D_E, which consists of declarations for all variables preserved by π. The path therefore preserves all variables preserved by π. If π progresses on X then $\chi(\pi)$ contains $[{+}X\,]$ in its prefix. Since this modifier is eliminated in the constructed derivation using the ($[{+}X\,]$) rule, the path must progress on X. □

Proof of Lemma 4.14. The proof goes by induction on k. The base case, $k = 1$, holds trivially. For the induction case, consider a process $\mathsf{Q}\,\mathsf{q}$ where q is not ε. Using $\Gamma = \{x : \Psi \mid \Psi \in \mathit{AS}(\mathbf{u},\mathsf{r})\}$, we have

$$\dfrac{\dfrac{\dfrac{\mathsf{D}_\mathsf{E}\,;\,\Gamma \vdash \mathsf{Q}\,\mathsf{q}\,x\!:\!\varphi}{\mathsf{D}_\mathsf{E}\,;\,\Gamma \vdash \mathsf{q}\,x\!:\bigwedge\{\Psi \mid \Psi \in \mathit{AS}(\mathbf{u},\mathsf{q}\,\mathsf{r})\}} \qquad \dfrac{\mathsf{D}_\mathsf{E}\,;\,\mathsf{q}\,x\!:\bigwedge\{\Psi \mid \Psi \in \mathit{AS}(\mathbf{u},\mathsf{q}\,\mathsf{r})\} \vdash \mathsf{Q}\,\mathsf{q}\,x : \varphi}{\mathsf{D}_\mathsf{E}\,;\,x\!:\bigwedge\{\Psi \mid \Psi \in \mathit{AS}(\mathbf{u},\mathsf{q}\,\mathsf{r})\} \vdash \mathsf{Q}\,x : \varphi}}{\{\mathsf{D}_\mathsf{E}\,;\,\Gamma \vdash \mathsf{q}\,x\!:\!\Psi\}_{\Psi \in \mathit{AS}(\mathbf{u},\mathsf{q}\,\mathsf{r})}} \qquad \mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in \mathit{AS}(\mathbf{u},\mathsf{q}\,\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi}{\vdots}$$

The leaf in the right-hand branch is $\mathcal{S}(\mathbf{u}, \mathsf{Q})$ and thus already has the required form.

We continue with the left-hand branch. Since each $\Psi \in AS(\mathbf{u}, \mathsf{q}\,\mathsf{r})$ is the characteristic formula of a play $\mathbf{u}\pi\mathbf{v}_\pi$ with $\mathbf{v}_\pi = (\mathsf{q}\,\mathsf{r}, \mathsf{E}_\pi, \psi)$, we can apply Lemma B.4 to continue the the derivation for each such Ψ:

$$\dfrac{\begin{array}{c}\vdots\\ \mathsf{D}_\mathsf{E}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{q}\,x\!:\!\Psi\end{array}}{\mathsf{D}_{\mathsf{E}_\pi}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{v}_\pi,\mathsf{r})\} \vdash \mathsf{q}\,x\!:\!\psi}\ \text{(Lemma B.4)}$$

This leaf is $\mathcal{S}(\mathbf{v}_\pi, \mathsf{q})$, and we use the induction hypothesis on this sequent to obtain a derivation tree having only leaves of the form $\mathcal{S}(\mathbf{v}_{\pi\tau}, \mathsf{Q}_\tau)$ for some V-play τ extending π, thus completing the construction.

It remains to show the assertion about progress and preservation. This is immediate for the path from $\mathcal{S}(\mathbf{u}, \mathsf{Q}\,\mathsf{q})$ to $\mathcal{S}(\mathbf{u}, \mathsf{Q})$. Any other path from the root to a leaf consists of two parts, the path from $\mathcal{S}(\mathbf{u}, \mathsf{Q}\,\mathsf{q})$ to $\mathcal{S}(\mathbf{v}_\pi, \mathsf{q})$ in the derivation tree above, and the path from $\mathcal{S}(\mathbf{v}_\pi, \mathsf{q})$ to $\mathcal{S}(\mathbf{v}_{\pi\tau}, \mathsf{Q}_\tau)$, for some τ, in the derivation tree obtained by the induction hypothesis. We note that the play $\pi\tau$ preserves X if, and only if, π and τ both preserve X; and $\pi\tau$ progresses on X if, and only if, π preserves X and at least one of π and τ progresses on X. Similarly, this property holds for the two parts of the path. This allows us to establish the required property for $\pi\tau$ and the composed path. □

Proof of Lemma 4.15. We construct a derivation tree for the sequent $\mathcal{S}(\mathbf{u}, \mathsf{Q})$ where $\mathbf{u} = (\mathsf{Q}\,\mathsf{r}, \mathsf{E}, \varphi)$ is a position in a V-play. The sequent rules are used to mimic the possible moves of any V-play $\pi = \mathbf{u}\mathbf{v}_\pi$. We consider all possible cases for φ:

- φ is $\mathtt{tt}$. Apply ($\mathtt{tt}$R) to get a derivation without leaves.
- φ is $\mathtt{ff}$. In this case Verifier is stuck. But $\mathbf{u}$ is a position in a play in which Verifier uses her winning strategy, hence she can always make a move. Thus, φ cannot be $\mathtt{ff}$.
- φ is $\varphi_1 \wedge \varphi_2$. Refuter chooses either of the conjuncts. For $\mathbf{v}_\pi = (\mathsf{Q}\,\mathsf{r}, \mathsf{E}_\pi, \varphi_1)$ and $\mathbf{v}_\tau = (\mathsf{Q}\,\mathsf{r}, \mathsf{E}_\tau, \varphi_2)$, this gives two V-plays $\pi = \mathbf{u}\mathbf{v}_\pi$ and $\tau = \mathbf{u}\mathbf{v}_\tau$. Applying ($\wedge$R) and Lemma B.4 gives the desired derivation:

$$\dfrac{\dfrac{\mathsf{D}_\mathsf{E}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi_1 \wedge \varphi_2}{\mathsf{D}_\mathsf{E}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi_1}\ \text{(symmetric case)}}{\mathsf{D}_{\mathsf{E}_\pi}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{v}_\pi,\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi_1}\ \text{(Lemma B.4)}$$

- φ is $\varphi_1 \vee \varphi_2$: Verifier uses her winning strategy to choose one of the disjuncts, say φ_1. For $\mathbf{v}_\pi = (\mathsf{Q}\,\mathsf{r}, \mathsf{E}_\pi, \varphi_1)$ we get a V-play $\pi = \mathbf{u}\mathbf{v}_\pi$. We have the following derivation:

$$\dfrac{\dfrac{\mathsf{D}_\mathsf{E}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi_1 \vee \varphi_2}{\mathsf{D}_\mathsf{E}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi_1}\ \text{(Lemma B.4)}}{\mathsf{D}_{\mathsf{E}_\pi}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{v}_\pi,\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi_1}$$

- φ is $[a]\varphi_1$. For each q with $\mathsf{Q} \xrightarrow{a} \mathsf{q} \in \mathcal{P}$, the position $\mathbf{v}_\mathsf{q} = (\mathsf{q}\,\mathsf{r}, \mathsf{E}_\mathsf{q}, \varphi_1)$ induces a play $\pi_\mathsf{q} = \mathbf{u}\mathbf{v}_\mathsf{q}$. We start the derivation using ($[a]$R) and (P_iL):

$$\dfrac{\dfrac{\mathsf{D}_\mathsf{E}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\![a]\varphi_1}{\mathsf{D}_\mathsf{E}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\}, \mathsf{Q}\,x \xrightarrow{a} y \vdash y\!:\!\varphi_1}}{\{\mathsf{D}_\mathsf{E}\,;\, \{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{q}\,x\!:\!\varphi_1\}_{\mathsf{Q}\xrightarrow{a}\mathsf{q}\in\mathcal{P}}}$$

  We continue the derivation for each q. If q is ε then we apply the rule (Axiom). This rule is applicable since, because of the form of π_q, the characteristic formula of π_q, which is φ_1,

must be an element of $AS(\mathbf{u}, \mathsf{r})$. Otherwise, if q is not ε then q can be written as $\mathsf{Q}_\pi\,\mathsf{q}_\pi$. We continue the derivation for each q in the following way:

$$\frac{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}_\pi\,\mathsf{q}_\pi\,x\!:\!\varphi_1}{\mathsf{D}_{\mathsf{E}_\mathsf{q}}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{v}_\mathsf{q},\mathsf{r})\} \vdash \mathsf{Q}_\pi\,\mathsf{q}_\pi\,x\!:\!\varphi_1}\ \text{(Lemma B.4)}$$

In this derivation, q may be a sequence of more than one nonterminal. In this case, Lemma 4.14 is applied to complete the derivation.

- φ is $\langle a\rangle\varphi_1$. Verifier uses her winning strategy to make a move from the position $\mathbf{u}$ to a postition $\mathbf{v}_\pi = (\mathsf{q}\,\mathsf{r}, \mathsf{E}_\pi, \varphi_1)$ for some q for which $\mathsf{Q} \xrightarrow{a} \mathsf{q} \in \mathcal{P}$. We let $\pi = \mathbf{u}\mathbf{v}_\pi$. The derivation starts with ($\langle a\rangle$R) and ($\mathsf{P_i}$R):

$$\frac{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\langle a\rangle\varphi_1}{\underline{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x \xrightarrow{a} \mathsf{q}\,x} \qquad \mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{q}\,x\!:\!\varphi_1}$$

We continue with the right-hand branch in exactly the same way as in the case for $[a]\varphi_1$.

- φ is $\mu X.\,\varphi_X$. Verifier uses her winning strategy to choose a move from $\mathbf{u}$ to a position $\mathbf{v}_\pi$ of the form $(\mathsf{Q}\,\mathsf{r}, \mathsf{E}_\pi, \varphi[\,\mu X.\,\varphi_X\,/\,X])$. This gives a play $\pi = \mathbf{u}\mathbf{v}_\pi$, for which we have the following derivation:

$$\cfrac{\cfrac{\cfrac{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\mu X.\,\varphi_X}{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\langle X \leqslant \varphi_X\rangle\,\varphi_X}}{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi_X[\,\mu X.\,\varphi_X\,/\,X]}}{\mathsf{D}_{\mathsf{E}_\pi}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{v}_\pi,\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi_X[\,\mu X.\,\varphi_X\,/\,X]}\ \text{(Lemma B.4)}$$

- φ is $\nu X.\,\varphi_X$. In this case, let $\pi = \mathbf{u}\mathbf{v}_\pi$ for $\mathbf{v}_\pi = (\mathsf{Q}\,\mathsf{r}, \mathsf{E}', \varphi_X)$ where E' is $\mathsf{E},\ X = \varphi_X$. This play π does not preserve X, it preserves all other fixed-point variables, and does not progress on any variable. The characteristic formula $\chi(\pi)$ is thus $[X \geqslant \varphi_X\,]\,\varphi_X$, and the following is derivable:

$$\cfrac{\cfrac{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\nu X.\,\varphi_X}{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\![X \geqslant \varphi_X\,]\,\varphi_X}}{\mathsf{D}_{\mathsf{E},X=\varphi_X}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{v}_\pi,\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi_X}\ \text{(Lemma B.4)}$$

- φ is X. In this case, by definition of the position of a play, we know that the last definition in E is $X = \varphi_X$. We use the play $\pi = \mathbf{u}\mathbf{v}_\pi$ where $\mathbf{v}_\pi = (\mathsf{q}\,\mathsf{r}, \mathsf{E}, \varphi_X)$. The characteristic formula of π is $[+X\,]\,\varphi_X$, which justifies the following derivation:

$$\cfrac{\cfrac{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!X}{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{u},\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\![+X\,]\,\varphi_X}}{\mathsf{D}_\mathsf{E}\,;\,\{x\!:\!\Psi \mid \Psi \in AS(\mathbf{v}_\pi,\mathsf{r})\} \vdash \mathsf{Q}\,x\!:\!\varphi_X}\ \text{(Lemma B.4)}$$

The assertion about progress and preservation follows in the same way as in Lemma 4.14. □

Proof of Lemma 4.16. (Sketch) Let $\mathbf{u} = (\mathsf{p}, \mathsf{E}, \varphi)$ and $\Psi \in AS(\mathbf{u}, \varepsilon)$, i.e. Ψ is the characteristic formula of a play $\mathbf{u}\pi\mathbf{v}$ where $\mathbf{v}$ has the state ε. We start the derivation of $\vdash \varepsilon\!:\!\Psi$ with the elimination of the prefix of Ψ to arrive at a sequent of the form $\mathsf{D}\,;\,\vdash \varepsilon\!:\!\psi$. Note that this is a similar situation as in Lemma 4.15, but without the complication of process variables and the assumption set. In fact, the proof of Lemma 4.15 can easily be adapted for sequents of this kind. We can thus build a derivation-tree along V-plays for these epsilon-sequents. To this derivation, we can then apply the argument of Lemma 4.13 to show that this derivation-tree is indeed a proof. □